AUTHENTICATION ENHANCEMENT OF RFID CARD USING AN ELECTRONICALLY CLIPPABLE SHIELD AND FINGERPRINT-BIOMETRICS

IKUESAN RICHARD ADEYEMI

A dissertation submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Science (Information Security)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JANUARY, 2012

This dissertation is dedicated to my family for their endless support and encouragement, and particularly, to Philip and Samson Ikuesan.

ACKNOWLEDGEMENT

First and foremost, I would like to express my sincere gratitude to my supervisor **Dr. Norafida Binti Ithnin** for her unfading support, encouragement, and enlightenment through-out the period of this study, without whom, much effort would have been in vain and this project may have not seen fruition.

I would also want to appreciate all my colleagues in information security class, especially, those under the supervision of Dr. Norafida.

Special appreciation to all members of the Skudai Joy Gospel Chapel, a family that I will never forget.

Finally, I would like to appreciate all staffs of FSKSM, UTM and the entire UTM staff at large for the conducive learning environment.

ABSTRACT

Radio frequency identification (RFID) is a technology that employs basic identifier of an object embedded in a chip, transmitted via radio wave, for identification. An RFID Card, responds to query irrespective of '*Who*' holds the card; like a key to a door. Since an attacker can possess the card, access to such object can therefore be easily compromised. This security breach is classified as an unauthorized use of card, and it forms the bedrock for RFID card compromise especially in access control. As an authentication enhancement mechanism, this study designed and developed a method termed BIO-THENTIC Card, that integrates three existing mitigation methods which are physical clip tag, Faraday shield and fingerprint authentication; to prevent and also protect this weakness. The Bio-Thentic Card was fabricated, tested and assessed in line with the known threats, and attacks; and it was observed to proffer substantive solution to unauthorized use of RFID Card.

ABSTRAK

Pengenalpastian frekuensi radio (RFID) adalah teknologi yang menggunakan pengecam asas objek yang tertanam dalam cip, dihantar melalui gelombang radio, untuk pengenalan. Kad RFID, respons kepada pertanyaan tanpa mengira Siapa yang memegang kad seperti kunci pintu. Sejak penyerang boleh memiliki kad tersebut, akses kepada Oleh itu, objek itu boleh dengan mudah berkompromi. Pelanggaran keselamatan ini diklasifikasikan sebagai penggunaan tanpa kebenaran kad, dan ia membentuk batu hampar untuk berkompromi kad RFID terutama dalam kawalan akses. Sebagai mekanisme peningkatan pengesahan, kajian ini direka dan dibangunkan satu kaedah yang dipanggil BIO-Kad THENTIC, yang mengintegrasikan tiga kaedah mitigasi yang sedia ada yang tag klip fizikal, Faraday perisai dan pengesahan cap jari; untuk mencegah dan juga melindungi kelemahan ini. Kad Bio-Thentic direka, diuji dan dinilai selaras dengan ancaman yang diketahui, dan serangan; dan diperhatikan untuk mengajukan penyelesaian substantiative penggunaan tanpa kebenaran Kad RFID.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF EQUATIONS

CHAPTER 1

INTRODUCTION

1.1 Introduction

Radio frequency identifier (RFID) is one among series of wireless technology gaining faster and wider adoption in our today society. Unique to RFID is its portability, mobility, and flexibility in use. In a bid to make life much easier and simpler, this uniqueness has triggered its integration into our everyday life. Traditional way of identifying object/products in the retail industry; bar-code, is gradually being replace by the RFID. Of more importance to the adoption of RFID is its ability to be integrated into conveyor system, container, inventory, and transport tracking system, time sensitive application, self monitoring application such as expiry date alerts, and anti-counterfeiting of product. In addition, the relatively cheaper cost of the technology also contributes to such increasing demand.

Ironically, RFID unique properties have generated privacy concern and increasing security threats and attacks alike; which have attracted scholarly concern from researchers for the past two decades. Hence, various mitigations have been proposed to combat these challenges. Owing to the fact that the RFID system

constitutes four distinct layers (which are discussed in the following chapter), mitigations have also been structured to equate layer attacks. While the layers of the RFID system are been addressed, the physical-layer tends to receive less attention, and it has led to the success of most attacks. Researchers such as Juels (2006), Reiback (2005), Yahaya et al. (2010), e. t. c. have proposed measures to combat these attacks at the -physical-layer with focus on the reader-to-tag and tag-to-reader communication leaving the physical-layer vulnerable to unauthorized usage.

1.2 Problem Background

The adoption of RFID technology into areas like physical access control have generated questions such as; 'how can I know when my Card is being read', how can the Card detect the authentic owner of the Card. Series of such question have trailed the stage of RFID technology.

Yahaya et al. , (2009) proposed a framework upon which a Card can identify its authentic owner using a "biometric fingerprint match on Card" and a computer system for authentication. This is also similar to the model proposed by Fons et al. , (2006).

Marquardt et al. , (2010) proposed a controllable tag system. They modeled different types of tag that can be controlled by the user at will. This is also similar to the clipped tag designed by Moskowitz et. al. ,(2007).

Zanneti et al, (2010) proposed a "physical-layer identification" system of tag based on the principle of radiometry, which was termed PARADIS. They concluded that every tag has a unique fingerprint upon which they can be distinguished.

In all of the proposed mitigation however, the question of 'who' (how authentic is the authentic holder of the Card) authorizes the Card is yet to be answered. Zuo, (2010) concluded that the "survivability of the RFID system" should start from the security of each tag, noting that compromising attacks emanates from the tag. Langheinrich, (2008) identified "unauthorized tag readout" as the core of RFID privacy problem stating that authenticating the interrogating parties in RFID system is a technique for privacy concern.

Therefore, the challenge of authorized Card use and reading constitutes the bane of the security and privacy issues in the RFID system. Albeit, such challenges can be protected against by proposing an enhance authentication system particularly, at the user-end on the physical-layer of the RFID system.

1.3 Problem Statement

Attacks on the physical-layer of the RFID system have received minimum combative measure leading to the discouraging rate of attacks on it. Some of the existing measure tend to offer mitigation but failed to consider the authenticity of the user at the tag end of the system. Considering these limitations, satisfactory answers to the questions listed below needs to be purveyed in the process of this study:

i. How authentic is the authentic Cardholder?
ii. How can an authentic Cardholder dictate Card responds to interrogation?
iii. How can an authentic Cardholder know when the tag is being read?
iv. What happens to the confidentiality of the Card when it is stolen?
v. How will this proposed method be evaluated, with respect to authentic authorization?

1.4 Project Aim

The aim of this study is to improve the security level of the RFID system at the physical layer as well as ensure confidentiality in the use of RFID Cards by enhancing authentication of user at the tag end.

1.5 Project Objectives

In order to accomplish the aim of this study; the following objectives must be achieved:

i. To study and investigate existing mitigation measures on security and privacy of the RFID system with reference to the physical-layer.
ii. To propose an enhanced authentication mechanism for authenticating user at the tag-end of the RFID system
iii. To implement the proposed authentication mechanism and evaluate it effectiveness

1.6 Project Scope

The following defines the scope of this study:

1) This study entails security issues relating to the physical-layer of a passive and semi-passive tag used in contactless Cards.

2) The proposed enhancement method will be based on three existing mitigation methods, which are clipped tag, Faraday cage and fingerprint biometric authentication.
3) The designs and fabrication of the system is limited to the physics of the tag antenna and not on the detail of the RFID tag itself.

1.7 Significance of the dissertation

In this study, various mitigation measures for combating the challenges of the RFID system will be discussed. Furthermore, detailed analysis will be carried out on the specific three chosen measures, which will give insight to other researchers. The challenges of unauthorized tag read, tag use and even tag killing will receive appropriate mitigation.

1.8 Organization of report

This thesis comprises chapters arranged in the numeric other of 1 to 6. The detail of each chapter is detailed as follows;

Chapter 1 of this report gives the overview of this study, problem background, objective, scope, and problem statement of this study.

Chapter 2 of this report covers the history and basic theory of the RFID technology as well as its importance in various areas of application. Security and privacy challenges and existing mitigation in the RFID system were also discussed in detail.

Chapter 3 describes the research methodology of this study. In addition, it also discussed the project methodology for the study.

Chapter 4 of this report covers the design and fabrication process upon which the proposed methodology was framed.

Chapter 5 of this report discussed the result of the design and fabrication process. It also discussed result of risk assessment carried out on the fabricated prototype.

Chapter 6 covered the conclusion and recommendation proffered in this study.